e-ISSN: 2349-9745
p-ISSN: 2393-8161

Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

www.ijmter.com

A Review on Robust identity verification using signature of a person

Khyati P Goswami[1], Prof. Upen Nathwani[2]

[1,2]*Department of Computer Engineering, Noble Engineering College, Junagadh, Gujarat 362001,India.*

Abstract— Signature is behavioural type biometrics characteristics of human. Signature has been a distinguishing feature for person identification. In these days increasing number of transactions, especially related to financial and business are being authorized via signatures. Two types of verification methods are: Offline signature verification and online signature verification. In this paper we review various components of offline signature reorganization and verification system, feature extraction techniques and available techniques.

Keywords-Offline signature verification, types of forgery, feature extraction, FAR, FRR.

I. INTRODUCTION

Pattern recognition deals with the automatic detection and classification of objects and events. The interest in pattern recognition is so wide that pattern recognition applications attracts researchers and users belonging to all possible disciplines and areas ranging from business to the most sophisticated industrial applications. Robust system of recognizing and verifying signature is needed in a wide range of various banking and civilian applications that involves the use of cellular phones, passports, driver licenses and automatic teller machines[1].

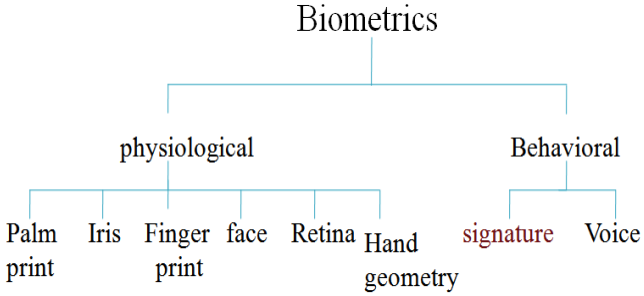

Fig. 1 Biometric technologies

Signature is a behavioral biometric. One's signature may change over time and it is not nearly as unique or difficult to forge as iris patterns or fingerprints, however signature's widespread acceptance by the public. This is primarily due to the age old and more usage of handwritten signatures as a means of personal or human identification and its freedom from association with any privacy leakage or intrusion related issues. Hence research in developing various biometrics systems that can improve the accuracy of these handwritten signature verification continues to be of very prime interest to date. However, it also has the demerits of lower verification and identification precision in comparison with all the other biometrics because of non-linear changes with size changing and its dependency on time and emotion [1].

Overall signature verification can be divided into two parts. Offline (static) signature verification and online (dynamic) signature verification. Off line signature verification make use of image of a signature which is put on the paper and then scanned by scanner. Online signature verification uses dynamic properties like pen downs and pen ups, signature trajectory, time stamping, pen pressure, etc.

Which are captured by a pen based tablet or device. Online signature verification is more reliable, robust, and accurate than offline signature verification as its overall dynamic properties makes the process of forging or copying an online signature more difficult. In real word these detail is too difficult to gather. It required lots of observation and detailed recording of it. Offline signature verification do not required any special hardware. It is simpler and user friendly than online signature verification system.[2]

II. TYPES OF FORGERY

Signature verification system based on the fact that signature of a person is unique. Signature verification system is used to authenticate a person's identity. It determines a genuine signature from a forgery. In offline signature verification signature is taken on a piece of paper and then scanned by scanner to convert it into digital form. [3]

Two signatures can be never same. Even it is done by the same person. even if two signatures are exactly same, then one of them is not a original signature but is a duplicate copy of the other that may be a machine copy, for e.g., one produced by a photocopier or computer, or a manually produced copy. So the aim of the signature verification system is to classify between two types: the original and the forgery. These classifications are related to intrapersonal variability and interpersonal variability. The variation of signatures of same person is called Intrapersonal Variation. The variation between genuine/original and forgeries is called as Inter Personal Variation. [3]

Forgery means that some person is trying to make false signature of some another person for authentication purpose. Forgeries are classified into three types [4]

1. Random/Simple Forgery: This is also called as simple forgery and it is very easy to detect as compared to others forgery. The person creates a signature in his own style by just knowing the name of a person whose signature is to be made.
2. Unskilled Forgery: The person creates a signature after observing the signature once or twice without any previous experience.
3. Skilled Forgery: The person may be a professional in making copy of signatures. He makes a signature after having a good practice over it. He may be expert in making forgeries. Such signatures are most difficult to detect.

To evaluate system's performance generally two types of errors are used. Type-I error and Type – II error. In type – I error genuine signature is falsely rejected by system. In Type- II error forged signature is accepted by system. These two errors are known as False Rejection Rate (FRR) and False Acceptance Rate (FAR). To measure or evaluate the performance of method, the term Equal Error Rate is used. Equal Error Rate is the point at which both FRR and FAR has the same value.[4]

III. WORKING SIGNATURE VERIFICATION SYSTEM

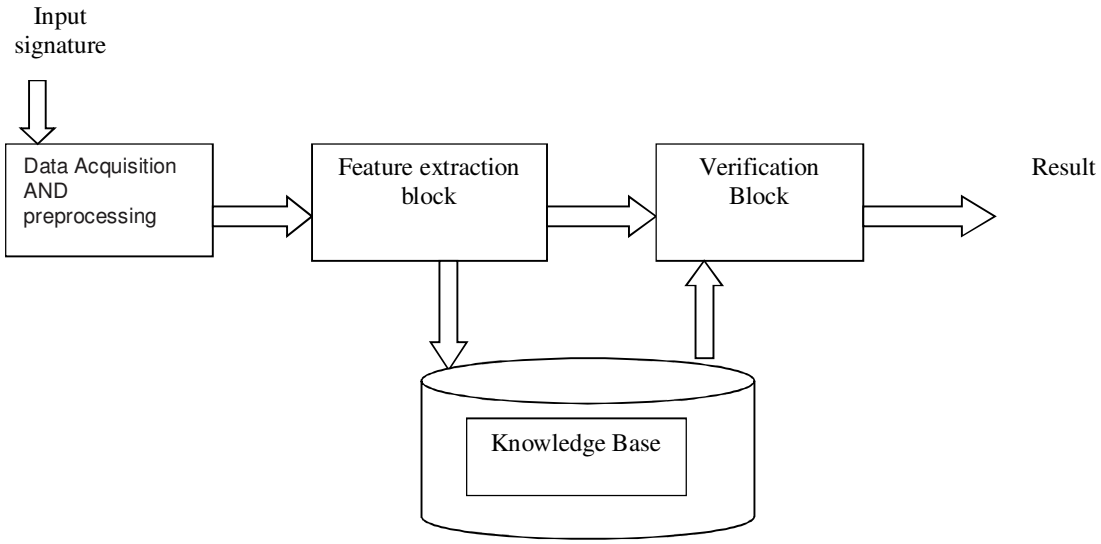

Fig: 2 Offline signature verification system

An offline SV includes generally four steps [4]:
1. Data Acquisition and Data pre-processing
2. Feature Extraction
3. Verification

A.Data Acquisition.

On the basis of how data is acquired, there are two categories of systems for signature verification: offline (static) systems and online (dynamic) systems. Static systems use offline acquisition tablets or devices that perform data acquisition after the whole signature writing process has been completed. In this case, the signature is represented as a gray level Image. Instead, dynamic systems use online acquisition tablets or devices that generate electronic signals that represents signature during the writing process.

B. Data Pre-processing

A pre-processing stage is done to improve the signature image after scanning it using a scanner device. This stage will influence the accuracy and reduce the computational time. This block may include Conversion from RGB to black and white image, inverting the image
, skew detection and correction, noise removal, signature cropping and image normalization (resizing), thinning the normalised image etc.

C. Feature extraction

It is the process of extracting the characteristics or attributes from an image. The accuracy of verification in pattern systems depends mainly on the extracted features. We can classify the signature verification systems in terms of extracted features into two kinds:

1. Global features

Global features describes the signature image as a whole like length, width, density, edge points of the signature, and wavelet transforms. These features are less sensitive to noise and signature variations. Global features may include Signature Height, Height-to-Width Ratio, Pure Width, Pure Height, Image Area, Maximum Horizontal Projection and Maximum Vertical Projection.

2. Local features

Which describe a small area of signature image and extract information in more details from it, it is more accurate than the global one but the computational time is high, it can be divided into two groups: statistical and geometrical features.
Statistical features: these are taken from pixel distribution of the signature image
Geometrical features: Geometrical features describe the geometrical characteristics of the signature image; Geometrical features have the ability to tolerate with distortion, style variations, rotation variations and certain degree of translation.

D. Verification

In this step, the reference features are compared with test features and signature is verified whether it is original or forges. Verification techniques usually divided into three parts which are: Template matching, Structural and Statistical. Template matching includes displacement function, Dynamic Time Wrapping, Euclidean distance. Structural approach includes String Graph Matching, Structural Description Graph etc. Statistical approach includes neural networks, hidden markov models etc. Out of these, most commonly used verification techniques are Neural Network, Hidden Markov Model and Support Vector Machine.

IV. RELATED WORK

Chuang [4] introduced a method for dividing the signature into three regions (upper, middle, and lower) out of which a number of global features were extracted. The features and their ratios were compared with those of the reference signature, using weighted distance as the dissimilarity metric. Chuang reports a 20% equal error rate for the proposed method. As can be inferred from the results of the systems, using only global image features is not sufficient.

H. Baltzakis [5] presented a new technique for offline signature recognition and verification. The proposed system is based on global, grid and texture features. For each one of these feature sets a special two stage Perceptron OCON (one-class-one-network) classification structure has been implemented. In the first stage, the classifier combines the decision results of the neural networks and the Euclidean distance obtained using the three feature sets. The results of the first-stage classifier feed a second-stage radial base function (RBF) neural network structure, which makes the final decision. The entire system was extensively tested with large amount of data and yielded a false acceptance rate is 9.81% and the false rejection rate is 3%. The implementation of neural network is very difficult and it takes more time to train the database.

Bradley Schafer [7] present an off-line signature verification and recognition system based on a combination of features extracted such as global features, mask features and grid features. The system is trained using a database of signatures. For each person, a centroid feature vector is obtained from a set of his/her genuine samples using the features that were extracted. The centroid signature is then used as a template which is used to verify a claimed signature. To obtain a satisfactory measure of

similarity between our template signature and the claimed signature, we use the Euclidean distance in the feature space. The results were very promising and a success rate of 84.1% was achieved using a localized threshold.

Debasish Jena [8] proposed Improved Offline Signature Verification Scheme Using Feature Point Extraction Method. The scheme is based on selecting 60 feature points from the geometric centre of the signature and compares them with the already trained feature points. these paper is improved version of scheme proposed by Banshider Majhi. FAR and FRR for proposed scheme gives improve result than existing scheme. There are few more feature extraction techniques available , we discuss only some of them

V. CONCLUSION

Offline signature verification system is easy to implement. Also it is highly adaptable. the ease of embedding the system in a business, organization or industries, without excessively affecting existing operations.In this paper we presents Offline signature verification system's overview, stepwise each block's functionality. We classify offline signature verification systems in terms of extracted features type into local and global features and also we classify local features into statistical and geometrical features. We have tried to analyze and study various methods of offline signature verification and hence provide a somewhat literature platform.

REFERENCES

[1] Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004.*

[2] D. Impedovo and G. Pirlo, "Automatic Signature Verification: The State of the Art", IEEE transactions on systems, man, and cybernetics, vol.3S, pp. 609-635,200S

[3] Rahul Dubey, Dheeraj K Agrawal" Comparative Analysis of Off-line Signature Recognition: 2012 International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India

[4] Debasish lena, Banshidhar Majhi, Sarojkumar Panigrahy, Sanjay Kumar Jena, "Improved Offline Signature Verification Scheme Using Feature Point Extraction Method", Proc. 7th IEEE In!. Conference. On Cognitive Informatics, pp. 475 - 4S0, ICCI 200S.

[5] P. C. Chuang, "Machine Verification of Handwritten Signature Image", *Inn Proceedings of International Conference on Crime Countermeasure, pp. 105- 109, 1977.*

[6] H. Baltzakis, N. Papamarkos, "A new signature verification technique based on a two-stage neural network classifier", *Engineering Applications of Artificial Intelligence 14,pp.95-103,2001.*

[7] Bradley Schafer, Serestina Viriri," An Off-Line Signature Verification System" *International Conference on Signal and Image Processing Applications*, pp.95-100,2009.

[8] Debasish Jena, Saroj Kumar Panigrahy,"Improved Offline Signature Verification Scheme Using Feature Point Extraction Method", *7th IEEE International Conference on Cognitive Informarics,* pp 475-480,2008.

[9] Shashi Kumar, K B Raja, R K Chhotaray," Off-line Signature Verification Based on Grid and Global Features Using Neural Networks", *International Journal Of Engineering Science and Technology*, Vol 2(12), pp 7035-7044, 2010.

[10] Piotr Parwik, " The compact three stages method of the signature recognition", *6th International Conference on Computer Information systems and Industrial management application* (CISIM'07), 2007..

[11] M.S.Shirdhonkar, Manesh Kokare," Off-line Handwritten Signature Identification Using Rotated Complex Wavelet Filters*", International Journal Of Computer Science*, vol 8, Issue 1,pp 748-753, 2011

[12] Mina Fakhalai, Hamid Reza,"off line signature recognition based on contourlet transform", *International Confernce on Machine Learning and Computing, vol.3,* pp 198-203,2011.

[13] Vu Nguyen, Graham Leedham,"Global features for the off-line signature verification problem ",*10th International Conference on Document Analysis and Recognition*, pp 1301-1304, 2009.

Shashi Kumar, K B Raja, R K Chhotaray," Off-line Signature Verification Based on Grid and Global Features Using Neural Networks", *International Journal Of Engineering Science and Technology*, Vol 2(12), pp 7035-7044, 2010.

